

Final Report

# Tactical ISDN Technology Program

30 September 1989

---

**Lincoln Laboratory**

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

*LEXINGTON, MASSACHUSETTS*



---

Prepared for the Department of the Air Force  
under Contract F19628-90-C-0002.

Approved for public release; distribution is unlimited.

ADA223813



This report is based on studies performed at Lincoln Laboratory, a center for research operated by Massachusetts Institute of Technology. The work was sponsored by the Department of the Air Force under Contract F19628-90-C-0002.

This report may be reproduced to satisfy needs of U.S. Government agencies.

The ESD Public Affairs Office has reviewed this report, and it is releasable to the National Technical Information Service, where it will be available to the general public, including foreign nationals.

This technical report has been reviewed and is approved for publication.

FOR THE COMMANDER

*Hugh L. Southall*

Hugh L. Southall, Lt. Col., USAF  
Chief, ESD Lincoln Laboratory Project Office

Non-Lincoln Recipients

**PLEASE DO NOT RETURN**

Permission is given to destroy this document  
when it is no longer needed.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY  
LINCOLN LABORATORY

**TACTICAL ISDN TECHNOLOGY PROGRAM**

*C.J. WEINSTEIN  
G.J. CHONCHOLAS  
G.C. O'LEARY  
Group 24*

*H.M. HEGGESTAD  
K.R. KOLODZIEJSKI  
Group 21*

FINAL REPORT  
TO THE  
ROME AIR DEVELOPMENT CENTER

1 OCTOBER 1988 — 30 SEPTEMBER 1989

ISSUED 21 MAY 1990

Approved for public release; distribution is unlimited.

LEXINGTON

MASSACHUSETTS

## **ABSTRACT**

This report describes work performed on the Tactical ISDN Technology Program sponsored by RADC/DCLD of the Department of the Air Force during the period 1 October 1988 through 30 September 1989.

## TABLE OF CONTENTS

ABSTRACT	iii
LIST OF ILLUSTRATIONS	vii
1. INTRODUCTION AND SUMMARY	1
2. THE AIR FORCE TACTICAL COMMUNICATIONS ENVIRONMENT	3
3. ISDN TECHNOLOGY STUDY	9
3.1 ISDN Overview	9
3.2 ISDN Course	11
3.3 ISDN Demonstrations	11
3.4 ISDN Products	12
4. DEVELOPMENT OF MILITARY APPLICATIONS OF ISDN TECHNOLOGY	15
4.1 Background	15
4.2 Work in Progress	15
5. DEVELOPMENT OF TACTICAL APPLICATIONS OF ISDN	17
6. ISSUES FOR SECURE ISDN COMMUNICATIONS	23
7. PLAN FOR ISDN TESTBED AND EXPERIMENTS	25
7.1 Testbed Description	25
7.2 Experiments	28
7.3 More Detailed Experiments	28
7.4 Future Uses	31
8. CONCLUSIONS AND FUTURE WORK	33
GLOSSARY	35
REFERENCES	37

## LIST OF ILLUSTRATIONS

Figure No.		Page
2-1	Environment for tactical Air Force communications	4
2-2	Minimum required connectivity for Tactical Air Control System (TACS)	5
2-3	Typical tactical switching hierarchy	6
3-1	ISDN model	10
5-1	Typical tactical switching hierarchy integration using ISDN	18
5-2	Application of ISDN/DGM gateway for ISDN node to ISDN node communications	20
5-3	Application of ISDN/DGM gateway for ISDN node to non-ISDN node communications	21
7-1	Interconnection of ISDN and TAC systems through gateways	26
7-2	Configuration for RADC ISDN testbed supporting interoperability experiments	27
7-3	ISDN testbed with capabilities for security experiments	29



## 1. INTRODUCTION AND SUMMARY

This report summarizes work carried out at Lincoln Laboratory during FY89 on a Tactical ISDN Technology investigation under AF/RADC sponsorship. The primary focus of the study has been to develop strategies for exploiting the features and capabilities of the emerging ISDN technology in order to meet the requirements for secure voice and data communications in a tactical environment. An important element of the effort has been to develop a plan for an ISDN testbed and experiments to support the future development of a Multi-Level Security Multimedia Integrated Service Network (MISEN). Efforts to date in this program have been described in three previous Quarterly Letter Reports, in a paper [8] presented at the October 1989 MILCOM Conference and in various briefings to RADC. This Annual Report replaces the fourth Quarterly Report, and summarizes work over FY89. The report covers the overall study effort, and includes a plan for the ISDN testbed and experiments.

In this effort, the features and capabilities of the emerging Integrated Services Digital Network (ISDN) have been investigated with the purpose of identifying ways to exploit ISDN technology to meet the demanding requirements of tactical communications. A study of the Air Force tactical communications environment demonstrates the need for robust, secure voice, data, and message communications over a geographically-dispersed network, where users move frequently and links are subject to jamming and to physical disruption. It is also essential that tactical facilities inter-operate with fixed military and commercial systems. Key problems identified with current tactical systems include: (1) high cost and limited flexibility due to the use of separate voice, data, and message switching facilities; and (2) inefficient utilization of limited transmission bandwidth, due to the prevalent use of fixed circuit allocations. ISDN offers a flexible, economical, standardized structure for voice and data communications, which has potential for application in addressing these problems. The following promising areas are identified for application of ISDN in the tactical environment: (1) integration of separate switches in a local area tactical facility such as a Tactical Air Control Center (TACC) into a common ISDN voice/data switch; (2) use of ISDN packet techniques and circuit switching techniques to efficiently multiplex traffic from a local area onto shared tactical links; (3) achievement of access from the local area to the tactical links by development of a gateway between an ISDN switch and the existing digital tactical transmission equipment; and (4) exploitation of the use of ISDN in a facility such as a TACC to expedite interoperation between tactical systems and commercial systems, which are beginning to widely utilize ISDN standards.

The U.S. Air Force Tactical Air Command (TAC) has a set of particularly demanding requirements for voice, data and record communications in support of its primary mission, which is to operate and control tactical aircraft at the forward edge of the battle area. The facilities involved in this mission include a fighter base and a Tactical Air Control Center well back of the lines (300–500 miles); Forward Air Control Posts close to the battle area; and a Combat Reporting Center in between. The people operating these sites need voice circuits to talk with each other and with the aircraft; data circuits to support digital data links to the aircraft and to other sites; and record traffic systems to distribute messages such as periodic Air Tasking Orders. These needs are

generally met today with three separate systems (voice, data, and message), and the costs are high by many criteria, including: initial investment, manpower requirements, flexibility, and bulkiness.

The Integrated Services Digital Network (ISDN) philosophy that is rapidly emerging in the commercial world [1,2] is working toward major savings in equipment size, complexity and cost by combining voice and data networks and services into a single set of facilities. International standards have been in the process of negotiation and acceptance for some time, and are giving rise to vigorous development in the commercial marketplace of equipment meeting these standards which will be competitively marketed to the operating companies. Such equipment is beginning to appear, and field tests are being conducted by a number of organizations. Although ISDN has primarily been applied for long-haul, fixed-plant communications, work is also being carried out to adapt ISDN-like protocols to mobile environments where bandwidth is limited [3].

Some of the capabilities that are beginning to be offered by ISDN closely resemble those required by the Tactical Air Force in many respects, and the opportunity exists to exploit commercial development activity to realize major cost savings in time and money for the Air Force. A study has been conducted with the objectives of: (1) describing and quantifying Tactical Air Force requirements; (2) researching both available and planned commercial ISDN service and equipment offerings, in the light of Air Force needs; (3) identifying unique military requirements which may be overlooked in present standards developments, so that these requirements can be factored in early in the process when this can be done economically; and (4) developing a plan for building a testbed in which emerging ISDN products can be evaluated in terms of military needs and applications. The ultimate objective of the study is to describe a future system architecture which will achieve the military needs. This report describes the tactical Air Force scenario, the goals and approaches being pursued in the study, the observations that have been carried out to date, and the areas in which it is expected that ISDN technology will be appropriate and valuable.

This report is organized as follows. Section 2 describes the Air Force tactical communications environment, with a view to identifying areas where ISDN technology could be useful. In Section 3, we give an overview of our study of commercial ISDN technology, and a summary of commercial products relevant to tactical communications. In Section 4, a number of DoD-sponsored efforts addressing military applications of ISDN are summarized. Section 5 describes new areas identified in the study as particularly promising for development of tactical applications of ISDN. Section 6 describes our preliminary work in ISDN security architectures. Section 7 describes our plan for an ISDN testbed and experiments. Brief conclusions are presented in Section 8. A separate glossary is provided to define in one place many of the TAC and ISDN acronyms used in this report.



## 2. THE AIR FORCE TACTICAL COMMUNICATIONS ENVIRONMENT

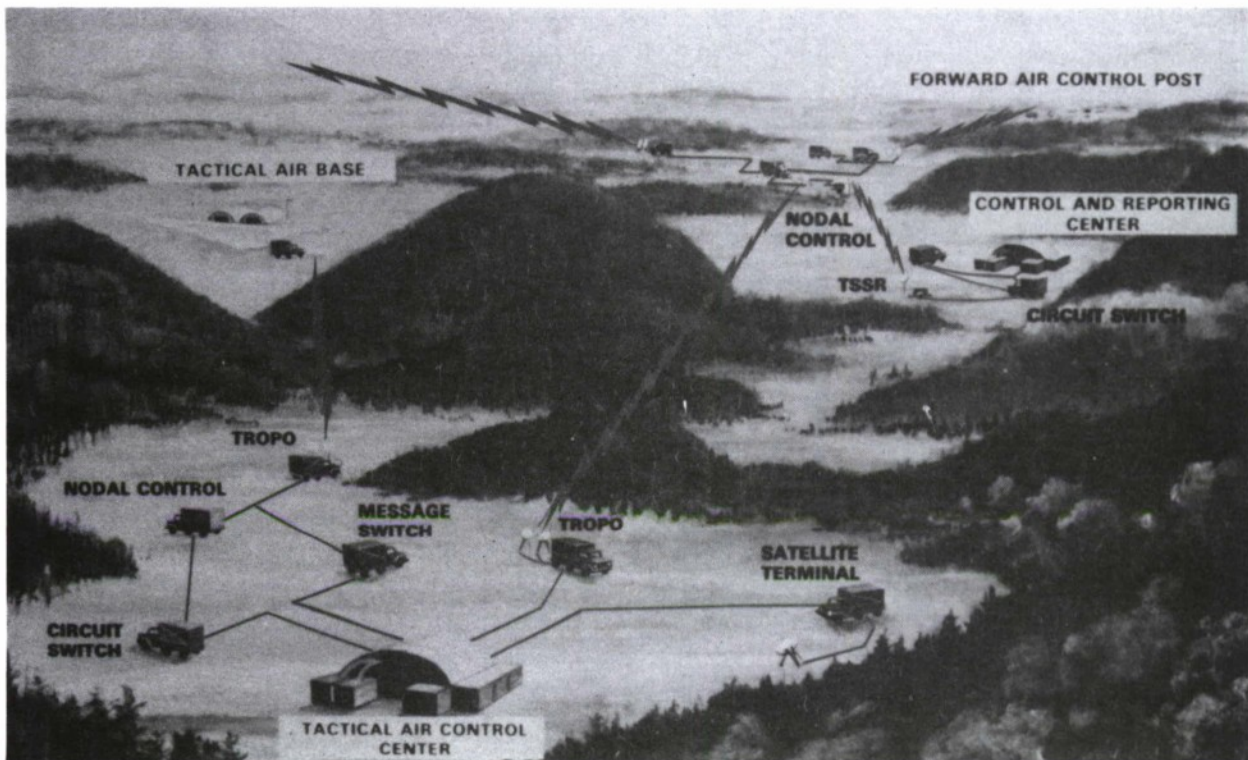
A typical environment for Air Force tactical communications is depicted in Figure 2-1. Operations from the tactical air base are directed from the nearby Tactical Air Control Center (TACC). The TACC also communicates outside the deployed environment depicted in the figure, to Tactical Air Force (TAF) Headquarters, to Airborne Command Posts (ABCP), and to joint forces and strategic facilities. In particular, Air Tasking Orders (ATO) are communicated periodically between the TACC and other tactical elements and command centers. As depicted in the figure, the TACC is served by separate switches for voice and message traffic. Transmission is provided by a mix of tropospheric-scatter radio and satellite media. In gathering and disseminating critical information and commands, the TACC must be served by robust, secure communication with a Control and Reporting Center (CRC) closer to the front, and with Forward Air Control Posts (FACP) near the battle zone. The control of the network must be distributed, so that it can survive damage of some of its elements. For flexibility, the hierarchy of communications may have to be bypassed at times; for example, CRCs may communicate with ABCPs, or with other elements outside the deployed unit.

A more detailed network model for TACS is shown in Figure 2-2, which indicates estimated minimum connectivity among TACS elements [8]. There is a heavy reliance on dedicated circuits. In the figure, the "V" links represent dedicated voice circuits; and the "D" links represent dedicated data circuits for teletype or FAX, which connect to the message switch in the TACC. Sharing of V and D circuits could make more efficient use of scarce bandwidth. The "T" label represent non-dedicated voice trunks connecting two circuit switches.

In the current tactical communications system, circuit-switching is provided by the TRI-TAC TTC family of switches, which generally operate on the basis of 16 or 32 kb/s voice digitization. Message switching is largely focussed on record traffic, which is essentially an electronic mail service. However, the need for fast data communications has greatly increased since the TRI-TAC system was designed. Handling this traffic on a circuit-switched basis is very wasteful of the limited transmission bandwidth available. The efficient integration of voice and data traffic into a unified switching framework would help to alleviate this capacity shortfall.

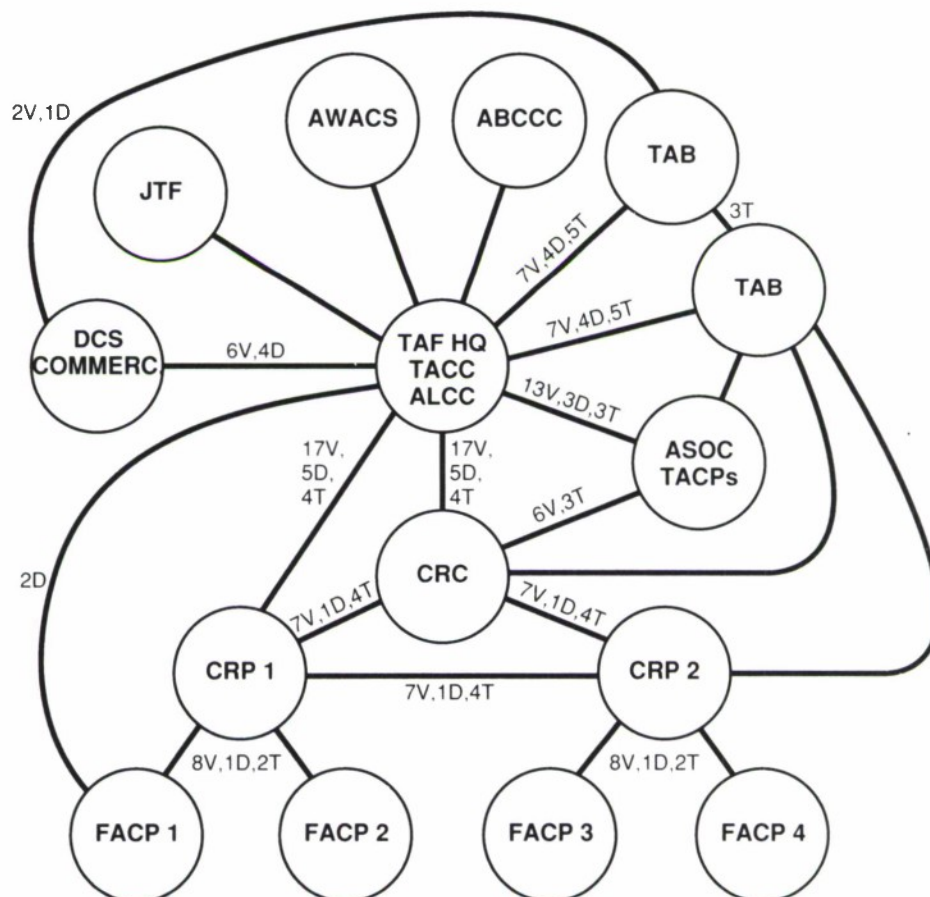
Figure 2-3 shows a typical tactical switching hierarchy that might appear at a TACC. Some of the elements illustrated are new developments which are not yet fielded. Note the variety of separate switches which are present, and the need for a channel bank to interface to the commercial network. Also, the proliferation of LANs and PCs has led to the need for a data switch to connect them to the circuit-switched network. With these layers of switches, a TAC operations officer with a phone and PC would require separate connections (via circuit switch and LAN) to the transmission network. In addition to the complexity and cost of separate connections, moves and changes are more difficult than necessary.

An additional requirement for tactical systems is interoperation with fixed DoD, commercial and allied systems. Specialized gateways are generally needed to achieve interoperation. More



144116-1

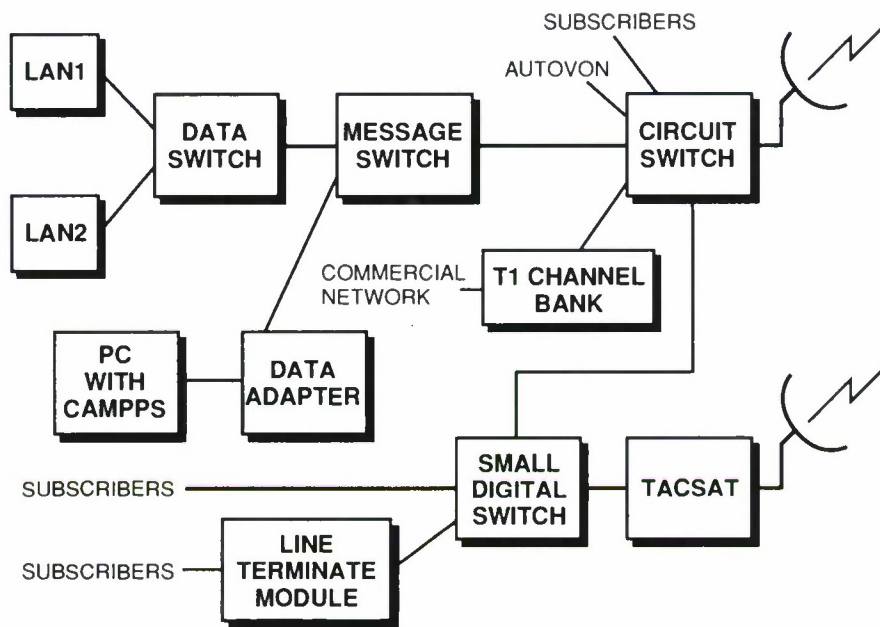
Figure 2-1. Environment for tactical Air Force communications.



V = DEDICATED VOICE CIRCUIT  
D = TELETYPE OR FAX CIRCUIT  
T = INTERSWITCH TRUNK

144116-2

Figure 2-2. Minimum required connectivity for Tactical Air Control System (TACS).



144116-3

Figure 2-3. Typical tactical switching hierarchy.



efficient interoperation, using a common set of transmission standards, would both facilitate communication with users outside the tactical environment, and allow tactical elements to utilize alternate link media (for example, through PTTs in Europe) to supplement the tropo links, which have limited bandwidth and are subject to jamming and disruption.

In order to further develop our TACS network model we visited the CRP in Worcester, MA, operated by the Air National Guard. The remainder of this section summarizes some of the information obtained from discussions with the Worcester personnel, and with other individuals knowledgeable in tactical communications. The two major functions of a CRC/P and a Forward Air Control Post (FACP) are tracking and identifying unknown targets and guiding aircraft from the tactical airbases to their mission. There are typically 4 radar scopes at a FACP and 14 at a CRC/P, where half the scopes are for tracking and identifying unknown targets and the other half are for guiding aircraft to their mission.

Air-to-air, air-to-ground, and FACP to CRP communication is by voice. When a CRC/P receives target data from the FACP via phone, it is manually entered into their radar scopes. Once entered, the data can be passed to other CRC/Ps using the TADIL B data system. If the CRC/P wishes to use a data format other than TADIL B, it must have Message Processing Center (MPC) equipment to perform the format conversion. For example, the Navy uses TADIL C and AWACS uses TADIL A.

Starting in FY90 the Air Force is deploying new equipment called Modular Control Equipment (MCE). The MCE AN/TYQ-23 operations modules (OMs) will replace the AN/TSQ-91 and AN/TSQ-61 currently in place at the CRC/P and FACP, respectively. When MCE is fielded, due to the benefits of automation and improved communications capabilities, the CRPs and MPCs will be eliminated. MCE will extend TADIL B out to the FACP and TACC, eliminating the need to transmit target information by voice. Each MCE OM will include four radar consoles.

The people we spoke with in Worcester suggested a number of aspects of tactical communications that could be improved:

1. Many incompatible protocols are used in tactical communications, necessitating much of protocol conversion equipment. This equipment adds weight and slows communication. Adopting a single protocol such as ISDN would eliminate these problems.
2. No maps or images were transmitted or received at this CRC/P. It would be useful to transmit weather maps and maps of the surrounding terrain. ISDN has services that could be used for this purpose, such as facsimile and slow scan video.
3. The present key distribution system can be improved. Key updating is unreliable, and the keys are on a paper tape which is subject to damage.
4. Key formats are often incompatible between services and commands.

### 3. ISDN TECHNOLOGY STUDY

As a part of our effort in this program, we needed to understand both the present and planned future capabilities of commercial ISDN technology. This section summarizes some of our studies in this regard. The section starts with an overview description of ISDN followed by a summary of an ISDN course we took in Boston. Then we describe ISDN demonstrations we have attended, and finally we summarize literature we have obtained and reviewed from ISDN equipment manufacturers.

#### 3.1 ISDN Overview

The public telephone network was originally designed to handle voice rather than data. Presently, data transmission requires a modem to make the data “appear” to be voice or requires a separate data network.

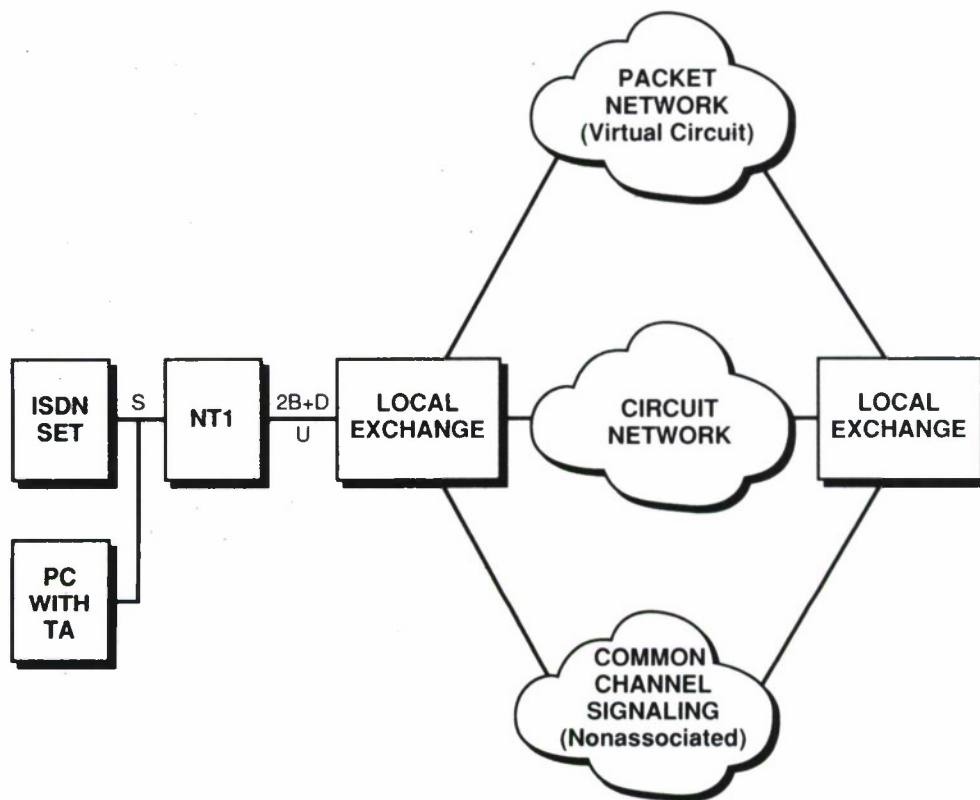
ISDN will become a worldwide public telecommunications network capable of handling voice and data simultaneously over the same transmission medium. The technology underlying ISDN has been driven by market pressures to reduce the cost of voice and data communications.

The ISDN is intended to provide multiple services on a common access facility. In the current network, the same voice services can be implemented differently on different vendor's Customer Premises Equipment (CPE). This forces the subscriber to buy equipment from a single vendor. ISDN would standardize the implementation of services allowing the subscriber to buy equipment from multiple vendors.

The ISDN is also intended to provide an end-to-end digital network with standardized interfaces and equipment. Today's network is generally analog from the subscriber's telephone to the PBX or central office and can convert multiple times between analog and digital when switching a call.

The most basic access to ISDN is the 2B+D channel illustrated in Figure 3-1. This channel has two 64 kb/s subchannels called Bearer (B) channels and a 16 kb/s subchannel called the Delta (D) channel. The B channels are used by the subscriber to place up to two simultaneous voice or data calls. The D channel is used for signalling such as call set up. The subscriber can also use the D channel for sending packet data when it is not being used for signalling.

The ISDN network itself can be considered to be composed of three subnetworks consisting of a circuit, packet, and common channel signalling network. A circuit-switched network provides a dedicated communication path between two stations through the duration of the call. The digital telephone network in place today is circuit switched. The packet network transmits data in short packets over a shared connection. Each type of network has its advantages and disadvantages. A circuit-switched network will block calls when all circuits are busy, whereas a packet network will not block calls, but will become congested with increased delays as traffic increases. A circuit-switched network uses a fixed amount of bandwidth for the duration of the call whether or not it is actually used, but a packet network uses bandwidth on demand. As a result, a packet network has more complex routing and congestion control problems than a circuit-switched network.



144116-4

Figure 3-1. ISDN model.

The common-channel signalling network is used to supervise calls. By separating the voice and signalling channel more services can be provided since they will not interfere with each other.

In short, ISDN is designed to standardize telecommunications services, interfaces, and equipment to provide a ubiquitous worldwide network. For an excellent, in-depth treatment of ISDN see [7].

### 3.2 ISDN Course

Four Lincoln personnel attended an ISDN course recommended by Philip Sykes of RADC. The course was called *Understanding ISDN*, presented by Telecommunications Research Associates, and given in Boston on February 28–1 March. The course started with a digital telecommunications overview, an overview of ISDN services, and a summary of the standards bodies. Next, we covered the ISDN reference points, functional groups and data rates.

Having defined the interfaces, we then studied the protocols on these interfaces. Specifically, we studied X.25 and Q.931 at layer 3, Q.921 at layer 2, and I.430 at layer 1. We also studied SS#7, which is used to provide ISDN services across switches. Finally, we discussed ISDN field trials and commercial products.

### 3.3 ISDN Demonstrations

We have toured the 5ESS switch at MIT and visited New England Telephone's ISDN customer demonstration site in Boston.

At MIT, we saw the main modules of the 5ESS in operation, including the 3B20 processors in the administration module and the switching modules that terminate their 5000 ISDN lines. We were interested in seeing a commonly-used commercial ISDN switch since the tactical communications network usually interfaces with the commercial network at some point.

At the New England Telephone demonstration site we were able to set up a simultaneous voice and data call through a live 5ESS switch. We also transmitted a document using Group IV FAX during a simultaneous voice call. The ISDN features demonstrated here are useful for tactical communications. Having simultaneous voice and data on the same pair of wires will reduce cabling time in the field and reduce the time to move equipment as the battle situation changes. The moves and changes services (which was not demonstrated, but was expected to be available soon) will further reduce the time to move equipment. The facsimile service would allow the transmission of weather and terrain maps. The D-channel used to control the demonstrated calls could also be used for key distribution. This would reduce the need to distribute paper keys which are prone to damage.

Northern Telecom has expressed willingness to meet with us to discuss their government and secure ISDN applications. Of particular interest at Northern Telecom is their system and ISDN hardware for secure communications [6], at their ISDN test and demonstration site.



### 3.4 ISDN Products

We have contacted ISDN equipment manufacturers requesting information on their products [12,13]. The companies who sent us information are listed below, with comments on the relevance of each product to our study.

- We contacted service providers regarding primary rate access between Lincoln and RADC and basic rate to our offices. This would allow Lincoln access to the National Institute of Standards and Technology (NIST) effort to connect government-sponsored ISDN test sites into a wide area network [9].

**AT&T** – Availability of primary rate access between Lincoln and RADC.

**US Sprint** – Availability of primary rate access between Lincoln and RADC.

**NYNEX** – Availability of basic rate access to our offices. This will become possible later this Fall when the system version in our local central office is upgraded.

- We contacted switch manufacturers to see which ISDN services have been implemented and if any switches would be suitable for an ISDN testbed. As discussed in Section 7, the Teleos switch appears to provide a good basis for an initial testbed.

**AT&T** – A range of products focusing on the 5ESS.

**Northern Telecom** – DMS 100 and SL PBX's.

**Teleos** – Adjunct processor and associated software for OEM applications.

**NEC** – ISDN adjunct system.

- We have also been monitoring ISDN terminal equipment. An interesting recent development is that Fujitsu and PictureTel Corporation of Peabody, MA, have demonstrated full-motion video and voice at 128 kb/s over two B-channels. This product would allow the transmission of video over the limited bandwidth of the tactical environment by doing image compression.

**AT&T** – ISDN sets, terminal adapters, NT1.

**Northern Telecom** – ISDN sets, terminal adapters, PC plug-in card.

**Fujitsu** – ISDN sets, terminal adaptor and image station.

**Mitel** – PC plug in card for product evaluation and as a teaching vehicle. The board is used for an ISDN course at Boston University.

**DGM&S** – PC plug-in card for OEM applications.

- A survey of VLSI chip sets for ISDN has been undertaken, to assess the range of products and the schedule for their availability. Professor D. Perreault of Boston University, who is studying ISDN chip set architectures in some detail under RADC sponsorship, has provided helpful input to our survey.

In terms of development schedule, we have found that the industry generally talks about a four-phase approach, of which Phase I was the pre-ISDN planning and standards development era extending from about 1983 to 1987, and Phase II was a trial phase for a small number of exploratory products in the 1987 to 1989 era. From 1988 through about 1993 is the “Limited ISDN Availability” phase, in which significant products will start to appear, while Phase IV, “General ISDN Availability,” is expected to begin in 1992 through 1993.

**National Semiconductor** – U and S interface devices.

**Motorola Semiconductor** – S/T transceiver.

**Advanced Micro Devices** – Subscriber S/T controller.

**AT&T** – S/T subscriber and network interfaces, U interface chip set.

**Mitel Semiconductor** – R, S, and U interface.

**Intel** – S/T controller.

- CACI Comnet II.5 is a telecommunications network analysis tool that can simulate ISDN networks. It runs on an IBM PC or Mac II. We may want to use this product to simulate how ISDN would perform in a tactical scenario.
- Below is a list of ISDN test equipment manufacturers, who provide a variety of equipment for test and maintenance of ISDN systems.

**Tekelec** – Chameleon 32 is an ISDN test system.

**Alelco** – BRI protocol analyzer including Q.931 and Q.921.  
SS#7 protocol analyzer.

**Digilogic** – HDLC/X.25 protocol analyzer.

## 4. DEVELOPMENT OF MILITARY APPLICATIONS OF ISDN TECHNOLOGY

### 4.1 Background

U.S. military communications systems, as they exist today, are the result of evolution over many years, through successive procurements. Great improvements could be made through modernization, but progress toward this goal is slow because budgets are perennially tight.

The anticipated development of ISDN technology has been welcomed by military communications planners as a way of achieving modernization at reasonable cost. Commercial products implementing ISDN features, such as sharing a single pair of wires among multiple voice and data circuits, are suitable for many military applications. With the development costs for these products being borne by private industry, and with mass production driving down their unit prices, it is in the Government's interest to take advantage of them. A number of DoD-sponsored efforts are underway to study the applicability of expected ISDN products in military problems, as well as to influence the development of ISDN standards and plans to better accommodate military needs. Part of the study effort reported in this paper has been concerned with surveying and keeping abreast of these efforts, and also in interacting with the individuals doing the work.

### 4.2 Work in Progress

The following paragraphs briefly describe a representative sampling of ongoing activity aimed at exploiting the developing ISDN for military purposes. The first three examples are technology development and evaluation efforts; the fourth describes Department of Defense (DoD) initiatives to influence standards development; and the fifth is a major military upgrade that is already beginning.

**RADC ISDN Testbed** The Air Force Rome Air Development Center (RADC) is building an ISDN Testbed. This work is founded upon the expectation that ISDN capabilities will meet many developing DoD needs within the Defense Communications System (DCS), which includes the entire DoD complex of voice and data networks. The overall goal of the RADC ISDN Testbed effort is to address specific issues by demonstrating real voice/data/image applications, identifying areas where extensions or revisions may be needed in order to satisfy military objectives. A phased implementation of the testbed is in progress. The first phase is based upon DGM&S Terminal Emulator boards and MITEL ISDN boards in a network of IBM PCs, constituting an actual ISDN Basic Rate Access link that supports multiple voice and data circuits upon which other ISDN products will be demonstrated and evaluated.

**ISDN Net** The National Institute of Standards and Technology (NIST) is drafting a plan for an experimental ISDN network that will link government locations

nationwide [9]. Applications specified by the North American ISDN Users' Forum (NIU), also sponsored by NIST, will be tested on ISDN Net. The five most likely sites are: NIST headquarters; Griffiss Air Force Base, including the RADC testbed described above; Mather Air Force Base; Pensacola Naval Air Station; and Goddard Space Flight Center. ISDN Net will connect the five ISDN islands with primary rate access to the commercial ISDN network.

**ISDN IC Support and ISDN Link Error Monitor** RADC is sponsoring these two areas of effort in the Electrical Engineering laboratory environment at Boston University. The first is a study of the VLSI chip sets offered by several IC manufacturers which externally address ISDN requirements and standards, but internally may have unique architectures which are not necessarily well suited for military needs. The objective of this work is to identify those offerings which are best suited for incorporation in products for military use. The second area of effort is a project to develop an ISDN Link Error Monitor that performs a logically complete set of tests and can be used effectively by a relatively junior technician, particularly in the military environment.

**Expert ISDN Link Diagnostic** This Artificial Intelligence (AI) oriented work is sponsored by RADC at Clarkson University. The objectives are to identify the types of knowledge needed for ISDN fault diagnosis; to determine the feasibility of an Expert System for this purpose; and to devise a suitable Expert System architecture together with recommendations for associated tools and protocol enhancements.

**DoD ISDN Working Groups** In 1986 the DoD established a committee to plan for the transition of the DCS to ISDN. This committee [4] is headed by a high-level executive steering group, and includes two subordinate activities: an ISDN Systems Working Group and an ISDN Standards and Technology Working Group. Two more working groups are under consideration, one for security and one for requirements.

**NATO LINK1 ISDN Program** This is a large multi-year effort preparing for replacement of the existing NATO LINK1 tactical communications system [5] in Europe with modern facilities based on ISDN. The general notion is that the public telephone system, operated by the various national Postal, Telephone and Telegraph (PTT) agencies, can be accessed within a short distance of virtually any tactical military operations area of interest in Europe. By designing NATO communications systems to tie into the public system, great advantages in flexibility and survivability can be achieved. The European PTTs are progressing more rapidly than their U.S. counterparts in implementation of ISDN facilities, hence the planned LINK1 replacement system is strongly oriented toward exploiting ISDN capabilities.



## 5. DEVELOPMENT OF TACTICAL APPLICATIONS OF ISDN

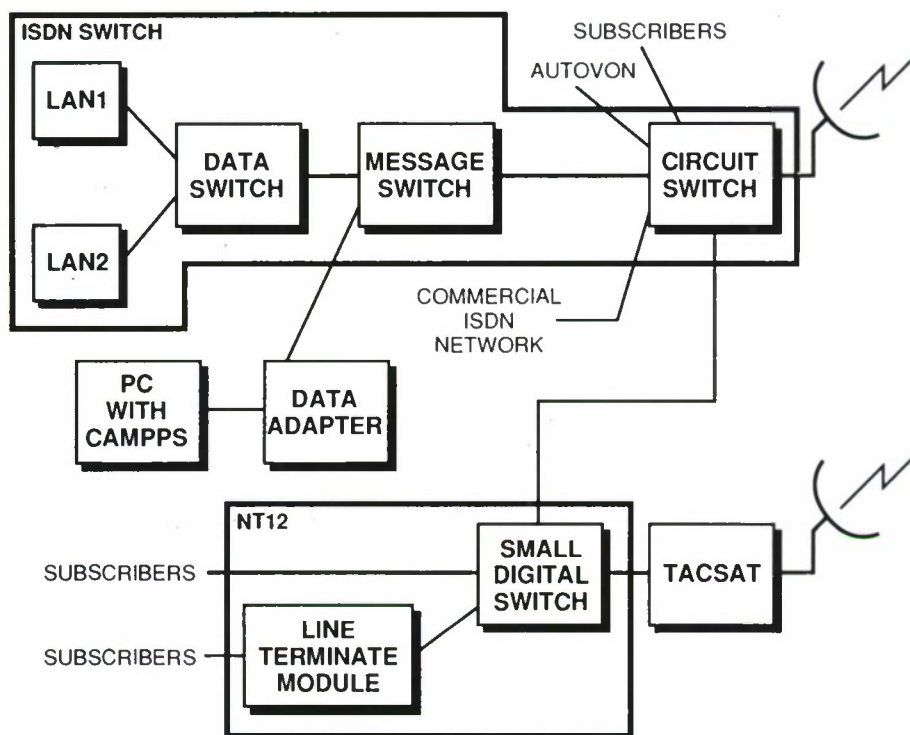
As noted in Section 2, we observe that the current TAC communications structure illustrated in Figure 2-1 is served by a circuit-switched voice network and a message-switched record traffic network that share transmission facilities, but otherwise require separate switches and separate user-level facilities at the various operations centers. Also, as noted above, there is a growing demand for higher-rate data transmission facilities operated over switched circuits (e.g., by use of modems on telephone lines), thus constituting a third network with overlapping and essentially inefficient use of resources.

The mapping of these TAC requirements into an ISDN environment is the focus of the current study effort, and the picture is not yet fully defined. There are encouraging indications, however, that the basic ISDN architecture may allow efficient satisfaction of all three TAC network applications noted above. In particular, the essence of the ISDN concept is flexible sharing of a single transmission circuit among multiple independent digital bit streams. In addition, ISDN switching technology provides the capability for integration of voice and data switching functions into a single switch.

With regard to the integration of switches, Figure 5-1 illustrates how an ISDN integrated access scheme could unify switching functions at a TACC. Here, a user with a phone and PC would have one connection to the switch. The standard integrated voice/data terminal interface which ISDN provides would greatly simplify the frequent moves and changes that occur at a tactical facility. The small digital switch (see Figure 2-3) can become, in ISDN terminology, an NT12 (combination of network termination 1 and 2), which provides the function of a PBX. Since the TACC would use an ISDN switch, direct interoperability with the commercial ISDN network would be provided.

With respect to efficient use of the limited transmission bandwidth in the tactical environment, ISDN switching can be helpful in the relatively short term only if compatibility with the existing TRITAC transmission equipment is established, since this transmission equipment is likely to remain in the field for many years. In particular, digital communications over tactical tropo radio and satellite links is multiplexed by Digital Group Multiplexers (DGMs) which are tightly coupled with the transmission equipment. Therefore, an attractive "target of opportunity" for application of ISDN in the TRITAC environment would be to design and develop an ISDN/DGM gateway to allow voice and data users in a local environment (e.g., TACC) to share tactical links without changing the DGM multiplexers. This would allow an evolutionary introduction of ISDN into tactical communications. Current tropo and SATCOM transmission equipment would remain unchanged as ISDN was phased into local area communications. The following discussion describes the DGM equipment and the ISDN/DGM gateway in more detail.

DGM is a family of equipment consisting of digital multiplexers, modems, control units for voice and data orderwires, repeaters for long cable systems and a field test set for their maintenance [14,15]. Virtually every TRI-TAC subsystem is equipped with some complement of the DGM family. The family consists of a hierarchy of digital multiplexers ranging from a low capacity portable field unit, which accepts up to four 16 kb/s or 32 kb/s user channels, to a shelter-mounted unit with a multiplexed output capacity of 1144 channels. A set of modems in the DGM family perform signal



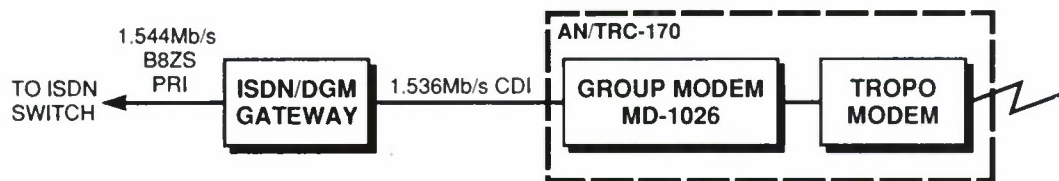
144116-5

Figure 5-1. Typical tactical switching hierarchy integration using ISDN.

conversion on the multiplexer aggregate signal for transmission over either coaxial or fiber optic cable, using conditioned diphase modulation and NRZ format, respectively.

The AN/TRC-170 troposcatter radio contains the following Digital Group Multiplexer equipment: one MD-1026 Group Modem (GM); two TD-1235 Loop Group Multiplexers (LGMs), or one TD-1235 LGM and one MD-1023 Low Speed Cable Driver Modem (LSCDM); and one TD-1236 Trunk Group Modem (TGM). The DGM equipment associated with the AN/TRC-170, listed above, can be configured for various applications. Figure 5-2 shows one interface structure to allow an AN/TRC-170 to be connected to local ISDN node (e.g., TACC) when the other node (e.g., CRC/P) is ISDN also. A gateway is needed for protocol conversion between the commercial ISDN switch and the TRI-TAC AN/TRC-170 radio because the ISDN Primary Rate Interface (PRI) data rate is 1.544 Mb/s with bipolar eight zero substitution (B8ZS) modulation and the DGM Group Modem is 1.536 Mb/s with conditioned diphase (CDI) modulation.

A more sophisticated gateway is required when AN/TRC-170s are used to communicate between an ISDN node and a non-ISDN node. In addition to having incompatible modulation, ISDN channels are 64 kb/s PCM and use out-of-band common-channel signalling, and Air Force tactical communications equipment is 32 kb/s CVSD with in-band signalling. As shown in Figure 5-3, the gateway must now perform multiplexing/demultiplexing functions to make the conversion between in-band and out-of-band signalling, along with changing between 32 kb/s CVSD and 64 kb/s PCM.



144116-6

*Figure 5-2. Application of ISDN/DGM gateway for ISDN node to ISDN node communications.*



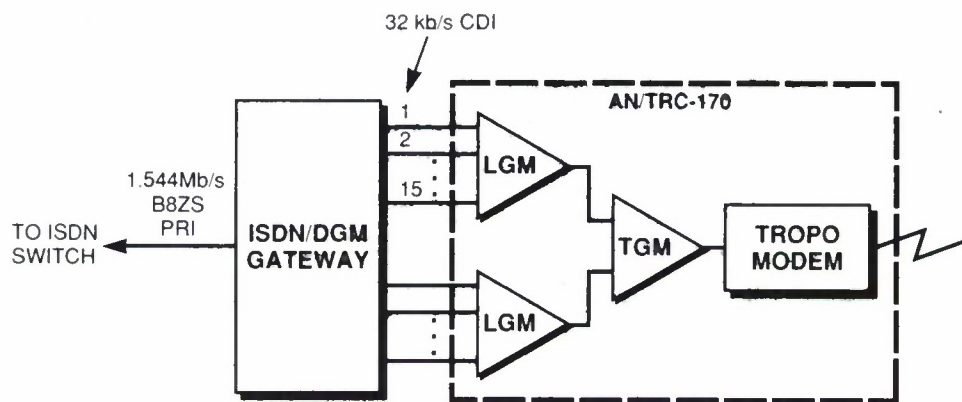


Figure 5-3. Application of ISDN/DGM gateway for ISDN node to non-ISDN node communications.

## 6. ISSUES FOR SECURE ISDN COMMUNICATIONS

If ISDN is to be useful for military communications, it must provide secure services. Presently, there are no official standards for security in ISDN; as a result, government agencies and corporations are collaborating to develop standards.

Our investigation of ISDN security architectures is in its preliminary stages. So far, we have attended the North American ISDN Users' Forum (NIU) in Boston, and investigated ISDN secure communications work being done at the NSA and Northern Telecom.

At the NIU we attended a session on ISDN security. They are using the International Standard ISO 7498-2-1988(E) as a guide for specifying secure services [11]. The NIU is developing ISDN standards for a number of the important security services, including authentication, access control, data confidentiality, and data integrity. It is important that the DoD continues involvement in developing secure services for ISDN because the standards are also being driven by nondefense industries. For example, the banking industry needs message authentication for electronic funds transfer and the securities industry needs message non-repudiation for confirming trades to a third party.

The NSA has started an effort called the Secure Data Network System (SDNS) that integrates state of the art cryptographic and key management algorithms into the existing OSI framework [10]. The program parallels the work being done by the ISO and NIU but relies on a more sophisticated system for key management. Eleven companies and several government agencies including NIST and the DCA are working on SDNS. SDNS devices are expected to become available in 1991. SDNS should be adaptable to ISDN since it conforms to the OSI model. The NSA is also testing a STU-III connection to an ISDN network through a commercial terminal adapter. The terminal adapter converts the STU-III tones to a 64 kb/s stream, and moves the inband signaling out of band to the D channel.

Northern Telecom at Bell-Northern Research is designing a secure ISDN telephone that connects to a normal NT1 [6]. The telephone looks like their M3000 touchphone. The user can choose to make secure or non-secure calls using the touch-sensitive screen. There is a large display area for prompting the user and for giving call status information.

The encryption strategy adopted is a hybrid between conventional and public key cryptography that combines elements of both. Public key encryption is used for the infrequent, block-oriented task of setting up session keys. The session keys are conventional keys in a stream cipher mode. The advantage of conventional stream cipher keys are they require less computation than public keys and do not need to accumulate an entire block of data before transmitting.

The D-channel out-of-band signaling is used to monitor and update key information while the B-channels are active. This prevents the communicating parties from having to call each other back after the appropriate keys have been obtained.

Our studies on secure ISDN systems began late in FY89, but this area is an important one for potential future work. The overall goal of a secure ISDN technology study would be to investigate

and develop the basic concepts of an ISDN security architecture for Air Force secure communication requirements. The study would include investigation of: (1) emerging technological trends and Air Force requirements in voice, data, and video transmission; (2) commercial ISDN technology including security mechanisms being developed for ISDN; and (3) corresponding security mechanisms for Air Force systems. A goal would be to develop an overall plan and specific techniques for matching and adapting ISDN technology to Air Force requirements for secure voice and data communications.

The work would build on the Tactical ISDN study reported here. Potential tasks for the secure ISDN technology study include:

1. Keep abreast of the security protocols and standards which are being developed for ISDN for commercial applications. Identify which of these meet Air Force requirements and which are inadequate. Study methods by which non-standard protocols can be added to meet these requirements.
2. Develop an architecture for a secure ISDN telephone modeled on the STU-III but providing 64 kb/s end-to-end connectivity, and allowing both voice and data communications.
3. Develop scenarios for secure conferencing with these telephones and with video terminals. Develop an architecture for a secure conferencing bridge which can accommodate all these devices. Investigate the issues involved in interoperable secure conferencing systems including ISDN terminals, STU-III terminals, and red switches in secure enclaves.
4. Develop architectures for systems which can demonstrate secure ISDN concepts and which can be incorporated into the RADC ISDN testbed. Design security experiments for this testbed help carry out these experiments and analyze the results.
5. Examine the unique Air Force problems related to integrating the secure ISDN environment with the Air Force tactical communication systems.
6. Examine the impact of ISDN on the special requirements for command and control.

## 7. PLAN FOR ISDN TESTBED AND EXPERIMENTS

The purpose of this section is to describe the RADC testbed and its current and proposed elements, to describe the set of experiments and demonstrations which could be carried out in the short term, and to describe some possible long-term applications of the testbed.

The goals of the integration effort between ISDN and the tactical (TAC) communications system are to produce an integrated system which can take advantage of the technology and equipment developed by the ISDN community for commercial applications, and apply this technology to the special requirements of the Air Force tactical communications world. This would initially be through gateways which would provide interoperability between the two systems as shown in Figure 7-1. The ISDN network is an all-digital telephone network made up of ISDN switches and instruments. It will provide direct digital voice and data connectivity directly to the customers' premises. We envision that in the not-too-distant future there will also be secure phones modeled on the STU-III concept which will be able to take advantage of the ISDN capability. The tactical environment consists of a collection of militarized voice and data equipment connected by wirelines, radio links (typically tropo scatter), and satellites. To demonstrate interoperability these systems would be connected by a gateway which would make the necessary conversions.

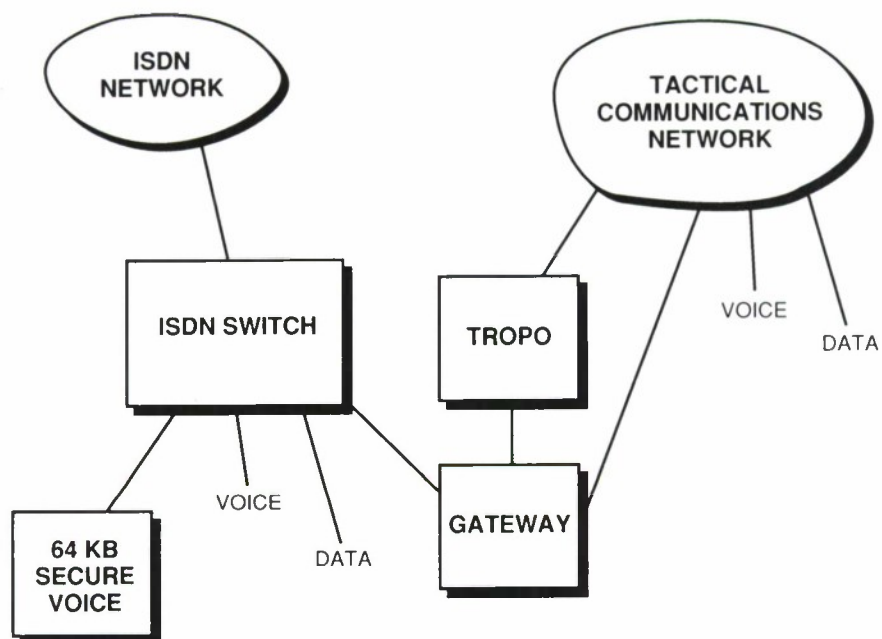
In the longer-range, new ISDN-based equipment could be developed for incorporation in the TAC communications network. This would make available to the tactical user the sophisticated services of ISDN. The techniques described in [3] could be adapted to develop ISDN-like protocols which would operate at bit rates well below 64 kb/s, as needed for many tactical AJ environments.

There are two primary experiment areas to which the testbed could be applied. The first is a broad set of experiments which demonstrate the interoperability of voice and data communications between ISDN and TACs. The second addresses the security issues involved in linking the security protocols, encryption equipment, and procedures of the two systems. This would include test and evaluation of new protocols for secure communication in ISDN.

### 7.1 Testbed Description

A possible starting point for a testbed for integrated ISDN/TAC experiments is shown in Figure 7-2. It would consist of an ISDN switch such as the Teleos switch at RADC with a collection of voice and data services interfaced through the Basic Rate (2B+D) interface lines. The tactical system would initially consist of a pair of Data Group Multiplexers (DGMs) connected to a tactical switch, and linked by a Tropo Link simulator. For initial experiments, the goal is to construct a gateway which can provide connectivity between the DGM and a standard interface on the ISDN switch. An initial interface demonstration would be done at basic rate (2B+D), with later efforts extending to primary rate (23B+D). As uses of the testbed progress, both the ISDN and tactical sides will be augmented with additional capabilities as required.





144116-8

Figure 7-1. Interconnection of ISDN and TAC systems through gateways.

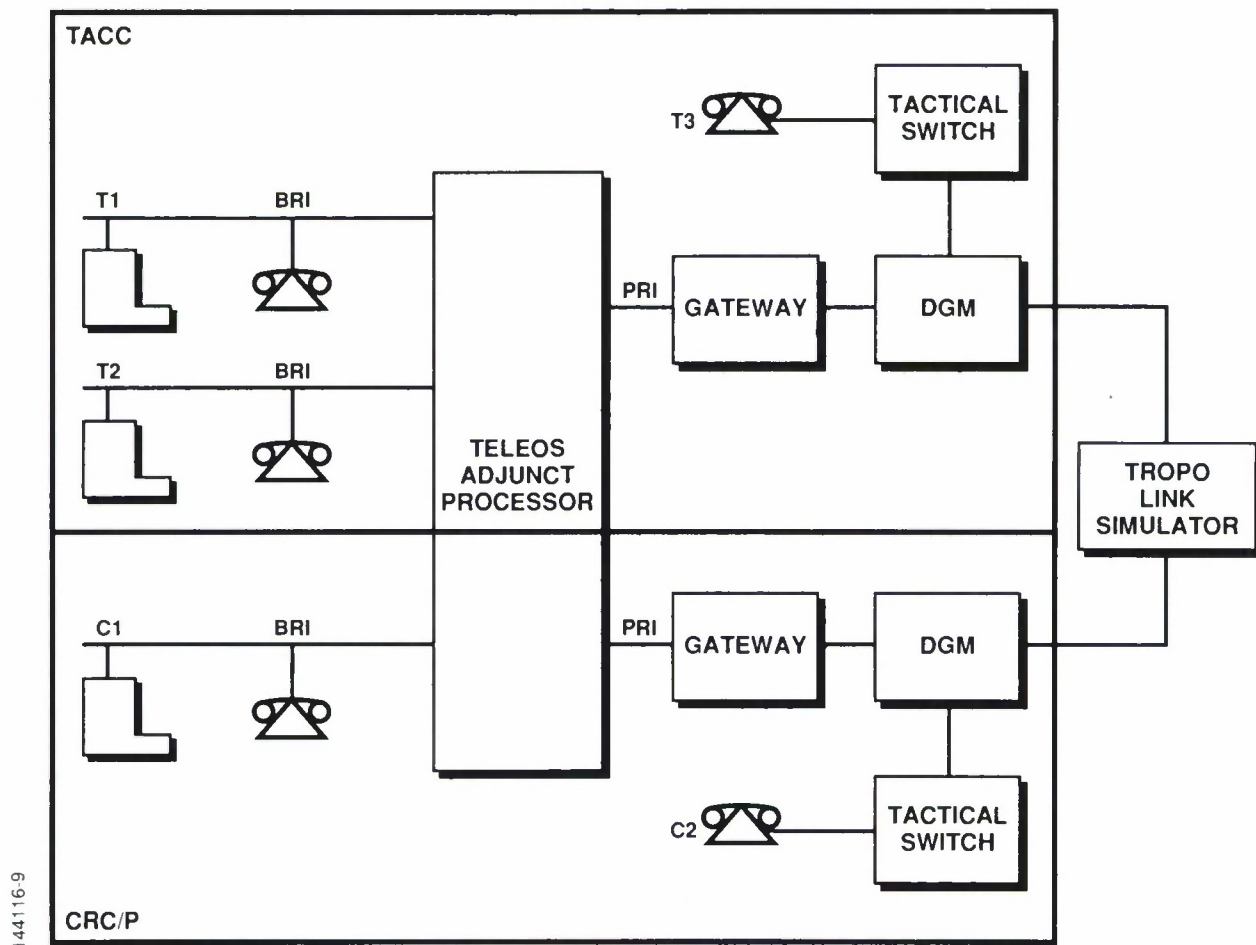


Figure 7-2. Configuration for RADC ISDN testbed supporting interoperability experiments.

## 7.2 Experiments

There are two primary experiment areas which need to be explored. The first is to demonstrate the interoperability of services between users in the ISDN and TAC systems. The second is to demonstrate the integration of security services and capabilities between the two worlds.

The interoperability will have to be demonstrated for both voice and data services. As a prerequisite to either, the conversion of signalling formats must be successfully performed. For voice, it will be necessary to automatically identify the connections with voice traffic and to perform the rate conversion between the 64 kb/s of the ISDN system and the 32 kb/s of the TAC system. For data connections, it will be necessary to demonstrate the necessary protocol conversions and provide the necessary rate conversion and its required data buffering.

Initially, security services in the ISDN system will be based on the current practice in the current telephone plant. This consists of voice systems such as the STU-III and data systems based on a variety of key generators. This equipment will have to interface to the TAC system with its own set of procedures.

Security experiments can be conducted at a number of levels. The most basic is to provide a RED enclave in which each of the signal is decrypted, converted, and encrypted again before transmission on the other network. At the next level experiments are needed to demonstrate the integration of the keying systems so that end-to-end encryption can be provided. Systems such as secure conferencing of the STU-III terminals will be extended to the tactical system. A third level will involve integrating and exploiting the security services which are being developed especially for the ISDN world. In addition, it will be important to demonstrate the interoperation of secure ISDN systems with current, secure Command and Control systems in the TAC environment. Demonstration of secure voice conferencing involving TAC  $C^2$  users, ISDN users, and STU-III users would be a key target experiment combining both security and interoperability features.

As an example of the application of the ISDN testbed shown in Figure 7-2, the upper and lower half networks might represent a TACC and a CRC/P, respectively. A non-secure call from T1 to C1, traversing the Teleos ISDN switch, the gateways, and the DGM multiplexers, would demonstrate use of tactical transmission facilities to carry ISDN calls. A call from T1 to C2 would demonstrate interoperation between ISDN and tactical terminals.

Figure 7-3 illustrates the introduction of security capabilities into the testbed. Modules would be introduced which provide ISDN-compatible security features compatible with the Secure Data Network System (SDNS) architecture currently being developed by NSA. Interoperability experiments would be performed, similar to those outlined above, but with the added security features, including simulation of basic key management center (KMC) facilities.

## 7.3 More Detailed Experiments

This subsection gives more detailed experiments for Figure 7-2. These experiments would demonstrate some of the necessary capabilities for communications between a TACC and a CRC/P using ISDN while interoperating with existing tactical equipment.

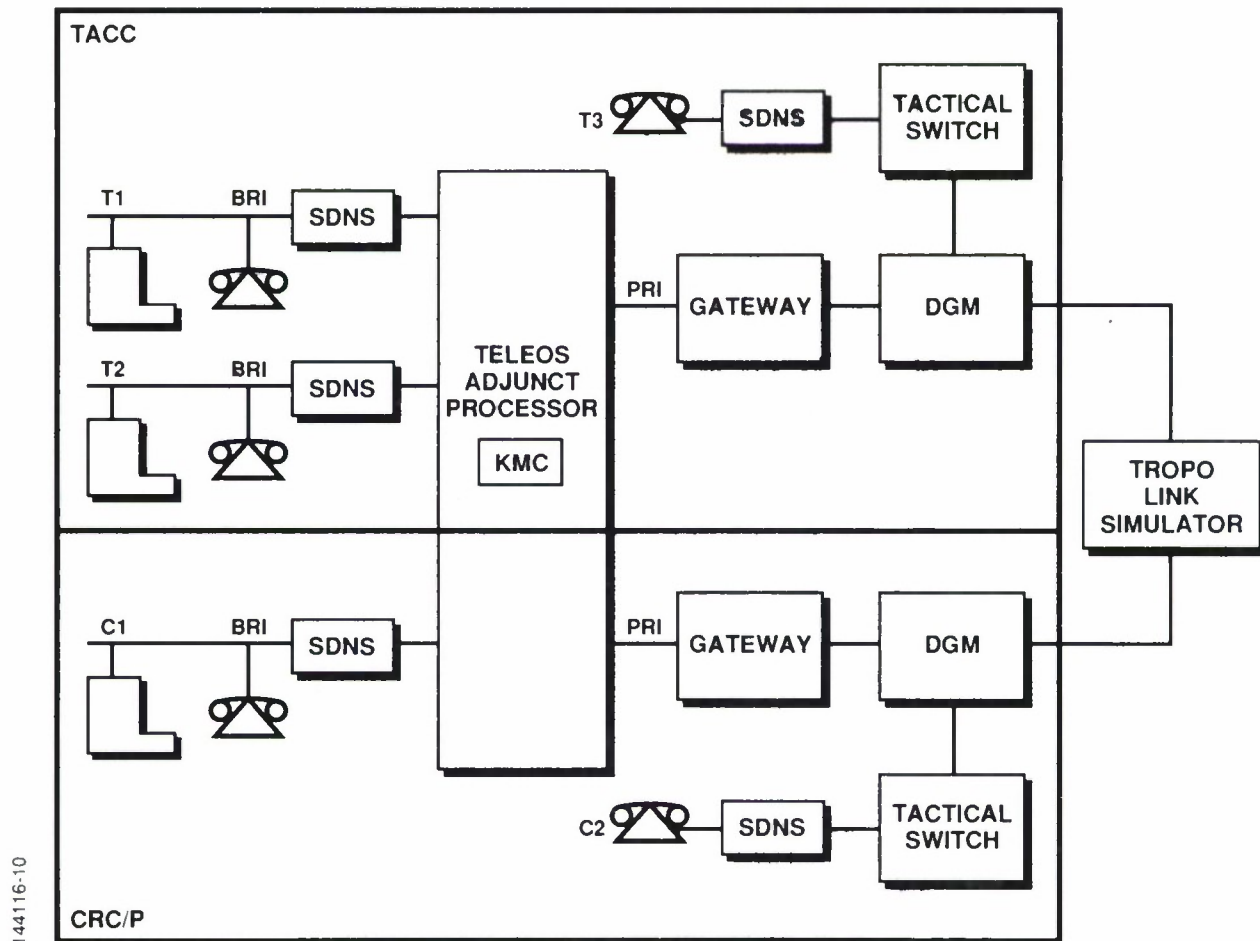


Figure 7-3. ISDN testbed with capabilities for security experiments.



Below are experiments that would ultimately lead to an ISDN-to-ISDN nonsecure voice call.

1. Connect the equipment to the right of the gateway and demonstrate a call between T3 and C2. This will demonstrate that existing tactical communications have been recreated successfully.
2. Demonstrate calls in an ISDN island, using the Teleos switch without any connections to the tactical equipment.
3. Join the tactical and ISDN islands created above using the top gateway in the figure. Set up a nonsecure voice call from T1 to C2. The gateway connecting the two islands would have to be designed to take the ISDN out-of-band signalling from the D channel and put it in band. In addition, the speech would have to be compressed from 64 kb/s down to 32 kb/s.
4. Implement a second copy of the gateway (lower gateway in the figure) and demonstrate an ISDN-to-ISDN nonsecure voice call from T1 to C1. This will show that signalling can be pulled back out-of-band and that speech can be expanded back to 64 kb/s.

Once nonsecure voice calls are demonstrated, circuit-switched nonsecure data calls can be demonstrated. Below are experiments to transfer a data file such as an Air Tasking Order (ATO).

1. Transmit a data file from T1 to C1 using the B channel. The file should be about the same size as a typical ATO. The first issue to be addressed, as for voice, is the bit rate incompatibility between the 64 kb/s B channel and the 32 kb/s tactical channel. Initially, ISDN data rates can be limited to 32 kb/s. The CCITT standards specify which bits are not used when using less than 64 kb/s. Later, experiments could be conducted in which two 32 kb/s tactical circuits are synchronized and multiplexed to form a 64 kb/s ISDN channel. Another issue to be addressed is that the gateway will have to distinguish between a data stream and a speech stream needing compression. The D channel can be used to make this determination when going from ISDN to tactical equipment. We have not solved the problem of making this determination in the reverse direction, where out-of-band signalling similar to the D-channel is not available at 32 kb/s.
2. Additional experiments could be conducted in transmission of images such as weather or terrain maps.

Next packets would be sent over the network. A packet could represent target information gathered at the CRC/P. The present tactical network does not have a separate packet network. The gateway would have to circuit switch the packets over the tropo link.

From here, secure communications would be introduced. The previous experiments could be repeated with secure voice and data. Then the testbed would be used to compare the ISDN security architectures that are emerging.

#### **7.4 Future Uses**

The testbed should be thought of as a long-term resource which will continue to track the evolving technologies and provide a way of quickly integrating them into the tactical arena. Besides the basic experiments describe above, the testbed can be used to test and demonstrate the tactical applications of new ISDN services as they become available. These include the graphics and image transmission equipment and capabilities of ISDN, which could have a significant impact on tactical communications capabilities.

## 8. CONCLUSIONS AND FUTURE WORK

Air Force tactical communications facilities serve a particularly demanding set of voice, data and message requirements. There is an opportunity to exploit the emerging commercial ISDN technology to modernize TAC communications, achieving increased efficiency in terms of cost, equipment complexity, and utilization of limited communication bandwidth. Several promising directions for application of ISDN technology to tactical communications have been identified. Goals of future work are expected to include: (1) further investigation of the tactical ISDN technology areas identified above; (2) development of a system architecture for utilization of ISDN in tactical communications; (3) development and experimental evaluation of a gateway between an ISDN switch and digital tactical transmission equipment, which will allow efficient multiplexing of communications traffic from a local area to tactical links; (4) development and experimental evaluation of an ISDN security architecture for Air Force tactical communications; and (5) further development both of a testbed system architecture and of a plan for exploiting that testbed to guide the evolution of the operational TAC communications structure.

## GLOSSARY

ABCC	Airborne Command and Control Center
ABCP	Airborne Command Post
ALCC	Airlift Control Center
ATO	Air Tasking Order
AWACS	Airborne Warning and Control System
CAMPPS	Computer Assisted Message Preparation and Processing Software
CRC	Control and Reporting Center
CRP	Combat Reporting Post
DCS	Defense Communications System
DGM	Digital Group Multiplexer
FACP	Forward Air Control Post
ISDN	Integrated Services Digital Network
LAN	Local Area Network
PBX	Private Branch Exchange
PC	Personal Computer
PTT	Postal Telephone and Telegraph Agency
T1	Standard Digital Carrier (1.544 Mb/s)
TAB	Tactical Air Base
TAC	Tactical Air Command
TACC	Tactical Air Control Center
TACS	Tactical Air Control System
TACSAT	Tactical Satellite



## REFERENCES

1. IEEE Journal on Selected Areas in Communications, Special Issues on ISDN, May 1986 and November 1986.
2. IEEE Communications Magazine, Special Issues Featuring ISDN, March 1986 and November 1986.
3. E.S.K. Chien, D.J. Goodman, and J.E. Russell, "Cellular Access Digital Network (CADN): Wireless Access to Networks of the Future," IEEE Commun. Magazine, Vol. 25, No. 6, pp. 22-31, June 1987.
4. J.J. Rudigier, "Army Implementation of ISDN," IEEE Commun. Magazine, Vol. 25, No. 12, pp. 44-49, December 1987.
5. C.L. Golliday, Jr., "Command and Control Systems," IEEE Trans. Selected Areas in Communications, Vol. SAC-3, No. 5, pp. 779-791, September 1985.
6. B. O'Higgins, W. Diffie, L. Strawczynski, P. de Hoog, "Encryption and ISDN— A Natural Fit," Proc. 1987 International Switching Symposium, Vol. 4.
7. W. Stallings, "ISDN: An Introduction", Macmillan Publishing Company New York, 1989.
8. C.J. Weinstein, H.M. Heggstad, and C. Meyer, "Tactical Applications of ISDN," IEEE 1989 Military Communications Conf., Boston, MA, October 1989.
9. "Feds Plan ISDN Net," ISDN Newsletter, Information Gatekeepers Boston, August 1989.
10. B. Karp, et al., "The Secure Data Network System," Defense Electronics, June 1989.
11. ISDN Security Services Definitions, North American ISDN Users' Forum, Implementors Security Working Group.
12. ISDN Handbook & Buyer's Guide, Information Gatekeepers, Boston, Second Edition, Volume 2, April 1989.
13. ISDN Handbook & Buyer's Guide, Information Gatekeepers, Boston, First Edition, Volume 1, April 1988.
14. Digital group multiplex (DGM) family, Raytheon, viewgraphs.
15. Tri-Tac DGM Equipment Manual.

## REPORT DOCUMENTATION PAGE

Form Approved  
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

[illegible]